Sustained Campaign Using Chinese Espionage Tools Targets Telcos

Attackers using tools associated with Chinese espionage groups have breached multiple telecom operators in a single Asian country in a long-running espionage campaign. The attackers placed backdoors on the networks of targeted companies and also attempted to steal credentials.

The attacks have been underway since at least 2021, with evidence to suggest that some of this activity may even date as far back as 2020. Virtually all of the organizations targeted were telecoms operators, with the addition of a services company that serves the telecoms sector and a university in another Asian country.

Tools used

Custom malware associated with a number of China-linked espionage actors was used in the campaign, including:

Coolclient: A backdoor associated with the Fireant group (aka Mustang Panda, Earth Preta). Its functionality includes logging keystrokes, reading and deleting files, and communication with a command and control (C&C) server. Variants of the backdoor used in this campaign were similar to one documented by Trend in 2023. A version of the legitimate VLC Media Player masquerading as a Google file (googleupdate.exe) was used to sideload a Coolclient loader (file name: libvlc.dll). The loader reads an encrypted payload from a file named loader.ja. This payload will in turn read a second encrypted payload from a file named goopdate.ja and inject it into the winver.exe process.

Quickheal: A backdoor that has been long associated with the Neeedleminer group (aka RedFoxtrot, Nomad Panda). The variant of Quickheal used in this campaign was a 32-bit DLL named RasTls.dll, which had an export named GetOfficeDatatal.

Analysis of the malware revealed that it was almost identical to Quickheal variants documented by Recorded Future in 2021, the only differences being new configuration details in the compiled code and VMProtect obfuscations.

The backdoor communicated with a hardcoded C&C server named swiftandfast.net using TCP port 443. It used a custom communications protocol that was designed to look like SSL traffic but used its own encryption instead.

Rainyday: A backdoor associated with the Firefly group (aka Naikon). Most of the Rainyday variants used during the campaign were executed using a loader named fspmapi.dll. The loader is sideloaded using a legitimate F-Secure executable named fsstm.exe. When loaded, it obtains the disk folder of the executable that started the process and sets it as the current directory. It then obtains the memory location of the executable and patches its memory image. This appears to be done in order to hijack the execution flow when the malware is loaded by a certain executable. If the hijack is successful, the loader reads from a file called dataresz, decrypts the payload with a single byte XOR key (0x2D) and executes it as shellcode.

Minor variants of the above include one with an invalid digital signature by "Kaspersky Lab" and another whose loader reads the encrypted shellcode from a file named iReports.

Another variant is executed using a loader named security.dll. It is sideloaded using an executable called msproxy.exe, which is an application called Proxifier, developed by Initex. The executable's default name is ProxyChecker.exe and was likely renamed to masquerade as a Microsoft file. In this case, the loader reads the encrypted shellcode from a file named nod193100. The XOR key used is also different: 0xF6.

Two files with the name nod193100 found on VirusTotal were, on analysis, found to be similar to a loader used for the Rainyday backdoor documented by Bitdefender in 2021.

Other TTPs

Aside from the custom backdoors mentioned above, the attackers used a variety of other tactics, techniques, and procedures (TTPs):

- Keylogging malware, possibly custom-developed
- Port scanning: At least three distinct port-scanning tools were deployed
- Credential theft through the dumping of registry hives
- Responder: A publicly available tool that acts as a Link-Local Multicast Name Resolution (LLMNR) NetBIOS Name Service (NBT-NS) and multicast DNS (mDNS) poisoner
- Enabling RDP

Links to Chinese Espionage Groups

Tools used in this campaign have strong associations with multiple Chinese groups and at least three of the custom backdoors deployed are believed to be used exclusively by Chinese espionage actors. Coolclient is tied to the Fireant group while Quickheal is associated with the Needleminer group. Rainyday, meanwhile, has always been used by the Firefly group. All three groups are widely considered by multiple security firms, including Symantec, to be operating from China. The United States–China Economic and Security Review Commission, an independent advisory body established by the U.S. Congress, has described Firefly as an "APT possibly associated with Unit 78020 (PLA) that operates in the southern theater command's area of responsibility (AOR)."

The nature of the link between the actors involved in the current campaign remains unclear. Possibilities include, but are not limited to:

- Attacks by multiple actors, acting independently of one another.
- A single actor using tools and/or personnel acquired from or shared by other groups.
- Multiple actors collaborating in a single campaign.

The ultimate motive of the intrusion campaign remains unclear. The attackers may have been gathering intelligence on the telecoms sector in that country. Eavesdropping is another possibility. Alternatively, the attackers may have been attempting to build a disruptive capability against critical infrastructure in that country.

Protection/Mitigation

For the latest protection updates, please visit the Symantec Protection Bulletin.

Indicators of Compromise

If an IOC is malicious and the file is available to us, Symantec Endpoint products will detect and block that file.

089809e73354648b3caed7db6bc24dcce4f2ef0f327206fd14f36c6619d9ed30 – Rainyday loader

1906e7d5a745a364c91f5e230e16e1566721ace1183a57e8d25ff437664c7d02 – Quickheal

3aae73ff8ff5973c74af5a7991ca6a57ce797b7b775e1358efd9d76b67b5797b – Rainyday loader

4c136270ca4c17edb77985aca570e291fa77abaaa48761f85e184892089164a6 – Coolclient

6a5fdbe9579b69d4a5e1f6930145debd5adb2a9f93dd052bfb442cbd0141277b – Coolclient

6ad67d7f76986359865667bdd51ba267f6bd7e560270512074448dd7b088bcb7 – Rainyday loader

c348eba51897fbd55ca3ffdaab21259b8f73688e6e008b923ebc597c6272d2d9 – Coolclient

c61daa0df88a33387b94b22bfc0b68d1211a57357aff401613c07832b5192fc0 – Rainyday loader

dc9a12574f8c3b5bed6043b1cd3fd43672779d132c864bb22ae8b0a5dee24576 –Rainyday loader

e32c5e6d70895f0d071f420b7ff28c6fe0eaf2c08eeebe39122b3b1fd1981473 – Rainyday loader f45dabd683795f099a40553e5d85c9bc8a15bb964c992b45cec48c620ff78fdb – Rainyday loader

103.180.161[.]123

110.34.166[.]198

203.159.95[.]197

115.79.207[.]240

206.189.140[.]171

117.2.82[.]149

113.160.186[.]153

134.209.147[.]60

139.59.35[.]77

134.209.156[.]5

139.84.137[.]139

139.84.130[.]178

139.59.37[.]50

139.84.165[.]248

139.84.166[.]131

139.84.163[.]162

14.161.4[.]152

142.93.223[.]200

146.190.18[.]167

143.110.250[.]11

143.110.244[.]132

159.65.158[.]28

159.89.170[.]164

157.245.107[.]16

38.60.254[.]243

43.152.200[.]62

206.189.136.180

65.20.66[.]128

49.204.77[.]162

65.20.66[.]214

65.20.69[.]80

65.20.70[.]110

65.20.82[.]212

65.20.73[.]72

65.20.76[.]211

swiftandfast[.]net